Amendments to the Claims:

1. (previously presented): A method of regulating access to a website by a user terminal via the internet, the user terminal reading a physical object including embedded steganographic indicia, said method comprising:

at the user terminal, extracting identifying data from the steganographic indicia, and providing the identifying data to a remotely located central computer;

at the central computer:

identifying a pointer associated with the identifying data;

generating at least one component of response information;

storing the response information; and

providing the pointer and response information to the user terminal;

at the user terminal, communicating with the website via the pointer and providing the response information to the website;

at the website, communicating verification information to the central computer; and

at the central computer, verifying authority to access the website based at least in part on a comparison of the verification information and the stored response information.

2. (previously presented): The method according to claim 1, wherein the identifying data comprises an object identifier.

3. (original): The method according to claim 2, wherein the pointer comprises at least one of a URL, IP address and web address.

4. (original): The method according to claim 2, wherein the at least one component comprises a random number.

5. (previously presented): The method according to claim 4, wherein said generating further comprises generating at least a second component, the second component comprising a time stamp.

6. (original): The method according to claim 2, wherein the response information comprises at least the random number and the time stamp.

7. (original): The method according to claim 6, wherein the verification information comprises at least the random number, the time stamp and a valid identifier.

8. (previously presented): The method according to claim 7, wherein said verifying authority comprises indexing the stored response information via the communicated random number and determining whether the stored response information matches the valid identifier and whether the verification information is received within a predetermined time period.

9. (previously presented): The method according to claim 8, wherein when the stored response information matches the valid identifier within the predetermined time period, said method further comprising authorizing user terminal access to the website.

10. (previously presented): The method according to claim 8, wherein when the stored response information does not match the valid identifier or the verification information is not received within the predetermined time period, said method further comprises signaling a lack of authority for the user terminal to access the website.

11. (previously presented): The method according to claim 7, wherein said verifying authority comprises indexing the stored response information via the valid identifier and determining whether a stored random number matches the communicated random number, and whether the verification information is received within a predetermined time period.

12. (previously presented): The method according to claim 1, further comprising encrypting at least one component of the response information.

13. (original): The method according to claim 2, wherein the document identifier is randomly generated.

14 -16. canceled.

17. (previously presented): A method of authenticating permission to access a system comprising:

receiving a request to enter the system, the request including at least a verification key, the request being associated with at least a steganographically marked object;

querying a data structure to determine whether the verification key is authorized; and

allowing access to the system based on the response to the query, wherein the verification key comprises a first random number, and the data structure comprises at least one data record including a second random number and a first identifier.

18. (original): The method according to claim 17, wherein the verification key further comprises a first time stamp and the data record further includes a second time stamp.

19. (original): The method according to claim 18, wherein said system communicates the first random number and a second identifier to the data structure, and wherein said data structure:

indexes the data record via the first random number, the first and second random numbers being equal,

determines whether the first identifier matches the second identifier, and whether the first time stamp is within a predetermined time range based on the second time stamp, and

signals to the system whether the first identifier matches the second identifier and whether the first time stamp is within the predetermined time range.

20. (original): The method according to claim 17, wherein the first identifier comprises an identifier extracted from a digital watermark.

21. (previously presented): The method according to claim 17, wherein said system communicates a second identifier and the first random number to the data structure, and wherein said data structure:

indexes the data record via the second identifier, the first identifier and second identifier being equal,

determines whether the first random number matches the second random number, and

signals to the system whether the first random number matches the second random number and whether the verification information is received within a predetermined time.

22. (original): A system for exchanging data comprising:

a central server comprising at least one database including response information and pointer information, wherein when a user terminal communicates an extracted watermark identifier to said central server, said central server identifies a corresponding URL with the extracted watermark identifier, and wherein said central server generates a number, and stores the number and extracted watermark identifier in the database as response information.

23. (original): The system according to claim 22, wherein said at least one database comprises a first database for storing pointers and a second database for storing response information.

24. (original): The system according to claim 22, wherein said server further generates a time stamp and stores the time stamp with the response information.

25. (original): The system according to claim 22, wherein the number comprises at least one of a random number, a pseudo-random number, and a predetermined number.

26. (previously presented): A method of operating a computer server, the computer server to communicate with at least one user terminal, said method comprising:

receiving an object identifier from the user terminal, wherein the object identifier is steganographically embedded in an object;

identifying a pointer associated with the object identifier, wherein the pointer comprises at least one of a URL, IP address and web address;

generating at least one component of response information;

storing the response information; and

providing the pointer and response information to the user terminal.

27. (previously presented): The method according to claim 26, wherein the object identifier is steganographically embedded in the form of a digital watermark.

28. canceled.

29. (original): The method according to claim 27, wherein the at least one component comprises a random number.

30. (original): The method according to claim 29, wherein the response information further comprises a time stamp.

31. (original): The method according to claim 26, wherein the response information comprises at least a random number and a time stamp.

32. (previously presented): The method according to claim 31, further comprising verifying data, wherein said verifying data comprises indexing the stored response information via a second random number, and determining whether the stored response information matches a valid identifier.

33. (previously presented): The method according to claim 32, wherein when the stored response information matches the valid identifier, said method further comprises authorizing user terminal access.

34. (previously presented): The method according to claim 32, wherein when the stored response information does not match a valid identifier, said method further comprises signaling a lack of authority for the user terminal.

35. (previously presented): The method according to claim 31, wherein said verifying data comprises indexing the stored response information via a valid identifier and determining whether the stored random number matches a second random number.

36. (previously presented): The method according to claim 31, further comprising encrypting at least one component of the response information.

37. (previously presented): The method according to claim 31, wherein the object identifier is randomly generated.

38. canceled.

39. (previously presented): A method of regulating access to a website by a user device over a network, the user device reading an object including hidden steganographic indicia, said method comprising:

receiving identifying data extracted from hidden steganographic indicia, wherein the identifying data was extracted by a remotely located user device and communicated via a network;

identifying a pointer associated with the identifying data, the pointer comprising information to access a website;

providing at least one component of response information;

storing the response information;

communicating the pointer and response information to the user device via the network, whereby the user device may access the website using at least the pointer and provide the response information to the website;

receiving verification information from the website including at least a portion of the response information;

verifying authority to access the website based at least in part on a comparison of at least a portion of the verification information and at least a portion of the stored response information; and

providing an indication of authority to the website.

40. (previously presented): The method of claim 39 wherein the indication inhibits access to the website.

41. (previously presented): The method of claim 39 wherein the indication allows access to the website.

42. (previously presented): The method of claim 39 wherein the user device comprises a handheld device.

43. (new): A machine-readable medium comprising instructions to perform the method of claim 39.